Remarks:

Applicant appreciatively acknowledges the Examiner's confirmation of receipt of Applicant's claim for priority and certified priority document under 35 U.S.C. § 119(a)-(d).

Reconsideration of the application is respectfully requested.

Claims 1 and 3 - 34 are presently pending in the application. Claim 21 has been amended. Claim 2 has been canceled. Applicant gratefully acknowledges that claims 15, 16 and 22 - 28 have been indicated as being allowable if rewritten to include all the limitations of the claims from which those claims depend.

In item 1 of the above-identified Office Action, the information disclosure statement was indicated as allegedly failing to provide a copy of DE 197 10 546 A1 and an English abstract for the same, which was listed as having been provided on Applicants' form 1449. Supplemental copies of DE 197 10 546 A1 and an English abstract are being provided herewith. A copy of the German search report received in the related German case and listing DE 197 10 546 A1, is additionally included herewith.

In item 2 of the Office Action, the information disclosure statement was indicated as failing to provide a concise

explanation of relevance or English translation of EPO 910 215 A2. A copy of an English abstract for EPO 910 215 A2 is provided herewith. EPO 910 215 A2 was cited as being a document "considered to be relevant" in an international search report issued in the related PCT application. A copy of that search report listing is additionally included herewith.

In item 3 of the Office Action, the disclosure was objected to because the specification recited a "CCD chip". The specification has been amended to replace the recitation of "CCD chip" with the phrase "charge-coupled device (CCD) chip". Similarly, in item 6 of the Office Action, claim 21 was objected to for reciting a "CCD chip". Claim 21 has been amended to replace the recitation of "CCD chip" with the phrase "charge-coupled device (CCD) chip". It is believed that these amendments address the objections made in items 3 and 6 of the Office Action.

In item 5 of the Office Action, claim 2 was objected to as allegedly being of improper dependent form, as allegedly being broader than claim 1, from which it depends. Claim 2 has been canceled.

In item 8 of the Office Action, claims 1 - 7 and 17 - 20 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U. S. Patent No. 6,792,287 to Tuomela ("**TUOMELA**").

In item 10 of the Office Action, claims 8 - 10 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over **TUOMELA** in view of U. S. Patent Application Publication No. 2002/0133716 to Harif ("**HARIF**"). In item 11 of the Office Action, claims 11 - 14 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over **TUOMELA** in view of U. S. Patent No. 6,271,745 to Anzai ("**ANZAI**"). In item 12 of the Office Action, claim 12 was rejected under 35 U.S.C. § 103(a) as allegedly being obvious over **TUOMELA** in view of U. S. Patent No. 6,628,810 to Harkin ("**HARKIN**").

Further, in item 13 of the Office Action, claims 29 - 34 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over **TUOMELA** in view of **ANZAI**.

Applicant respectfully traverses the above rejections.

Applicant's independent claim 1 recites, among other limitations:

> "assigning the user to one of several authorization levels based on the biometric fingerprint recognition; and
>
> **enabling at least one of a predetermined minimum range of functions and a predetermined minimum range of setting options of the appliance when** at least one of a biometric recognition failure occurs and **operation by an unknown user occurs.**" [emphasis added by Applicant]

Applicant's independent claim 29 includes similar limitations. As such, Applicant's claims require, among other things, that based on the biometric recognition of a user, one of several levels of authorization are assigned. However, Applicant's claims further require that **if an unknown user** (i.e., unrecognized user) **is determined, at least one of a predetermined minimum range of functions and a predetermined minimum range of setting options of the appliance** is still enabled. The advantages of Applicant's claimed invention are set forth in the instant application, in paragraph [0007], which states:

> "An inventive method for controlling a household appliance provides that a user is associated with one or more user and/or authorization levels by the biometric recognition. This opens up new areas of utility or new applications for biometric recognition beyond only two possibilities. **In the specific area of appliances, the possibilities of "user recognized" and "user not recognized" could only be associated with the actions "access granted" and "access denied".** It is possible to distinguish between an administrator with global authorization and subordinate normal users that way. Appliances that are equipped according to an inventive method are provided with a wide array of options for inputting control information based on defined characteristics of several user and/or

> authorization levels, which options will be separately discussed in connection with developments, various embodiments, and an exemplifying embodiment of the invention. Advantageously, selected settings of a user cannot be changed by any other user of the same appliance. In an embodiment of the invention, only a user who is higher in a hierarchy, such as a co-worker of a technician or someone who is otherwise furnished with maintenance authority, such as an administrator, is authorized to make modifications. **A predetermined minimum range of functions and/or setting capabilities is enabled given a failure of the biometric recognition and/or an operation by an unknown user. In a preferred embodiment, functions such as emergency shutdown can be executed by any user, including a non-registered user. This capability is not possible in methods according to the prior art based on upstream recognition as the authorizing process.**

As can be seen from the present application, it is disclosed that prior art systems worked such that if a user was recognized, they were provided with services; but if a user was not recognized, **they were not provided** with **any** services (i.e., "**In the specific area of appliances, the possibilities of "user recognized" and "user not recognized" could only be associated with the actions "access granted" and "access denied".**"). The present invention takes into account that a person who is not recognized as a user, may still require a minimum level of access to an appliance (i.e., "**In a preferred embodiment, functions such as emergency shutdown can be executed by any user, including a non-registered user.**"). This claimed enablement of limited functionality/setting options is **for the use** of the **unrecognized user**. Applicant's claimed system no longer presents a binary choice of **"access granted"** and **"access denied".**

Contrary to Applicant's claimed system, **TUOMELA** discloses an electronic apparatus, which although it may grant access to different users, each having their own profile, is of the binary, prior-art type when it comes to denying access. More particularly, **TUOMELA** primarily discloses a fingerprint recognition system intended primarily, but not exclusively for mobile phones in which a fingerprint recognition system recognizes the separate fingers and thumbs of a user and determines a function of the phone which has been previously associated with that recognized finger/thumb of the user. See **TUOMELA**, Abstract. Although, in col. 6 of **TUOMELA**, lines 60 - 67, it is stated that the invention of **TUOMELA** may be incorporated in other devices, including, among others, remote controls, televisions, washing machines and ovens.

TUOMELA additionally discloses in col. 5, line 65 - col. 6, line 7 and additional modification wherein each user would have their own user profile. Col. 5 of **TUOMELA**, line 65 - col. 6, line 7, states:

> "In one modification to the present invention, different users may be able to use the same telephone. Each user would have their own user profile. For example, with a mobile telephone belonging to a family, the parents may wish to prevent their children making certain types of calls. The user profile would be associated with one or more fingerprints of each user. **Thus when a user places a finger on the sensor plate 10, the user would be identified by his**

> **fingerprint and the telephone 2 would be arranged to operate in accordance with the identified user's profile."**

However, although **TUOMELA** may disclose giving **recognized users** their own user profile, in accordance with which, a telephone would operate, for unrecognized users, **TUOMELA** in the same "access denied" manner, as does the prior art.

This can be seen, for example, col. 5 of **TUOMELA**, lines 1 - 12, which states:

> "However in preferred embodiments, the fingerprint recognition system is also used as a security measure. **Thus in order for the user to be able to make a telephone call and/or to access information stored in a memory of the phone, a fingerprint of a user must be identified.** Thus the output of the second processor 20 is monitored. If a signal indicative of a match is output, then the user is able to dial a number and/or access information stored in the memory thereof. **If, on the other hand, the second processor 20 outputs a signal indicative that there is no match, then the user is unable to make any calls and/or access information stored in the memory.**" [emphasis added by Applicant]

The above described portion of **TUOMELA**, again, provides service to recognized users and **specifically teaches providing no service, as a security feature, to unrecognized users.** Providing **no service** to unrecognized users is very different from Applicant's claimed **enabling at least one of a predetermined minimum range of functions and a predetermined minimum range of setting options** of the appliance **when** at

least one of a biometric recognition failure occurs and **operation by an unknown user occurs**. Rather than enabling some minimum range of functions or settings when an unrecognized user is detected, **TUOMELA** specifically teaches **disabling** the functionality of the telephone. Applicant respectfully disagrees with the inference to be drawn on page 4 of the Office Action, first paragraph, that the disabling of functionality taught in **TUOMELA** is somehow analogous to Applicant's claimed **enabling of a predetermined minimum range of functionality/setting options**.

As such, Applicant's believe that, among other limitations of Applicant's claims, **TUOMELA** fails to teach or suggest, Applicant's claimed **enabling at least one of a predetermined minimum range of functions and a predetermined minimum range of setting options** of the appliance **when** at least one of a biometric recognition failure occurs and **operation by an unknown user occurs**. In fact, **TUOMELA** specifically **teaches away** from the above feature of Applicant's claims by stating that, **as a security measure,** if there is no recognition of a user **"then the user is unable to make any calls and/or access information stored in the memory"** (i.e., for unrecognized users, the phone of **TUOMELA** is disabled.).

In the Office Action, Applicant's independent claim 29 was rejected under a combination of **TUOMELA** and **ANZAI**. As discussed above, **TUOMELA** fails to teach or suggest Applicant's particularly claimed enablement of a predetermined minimum level of functionality/setting options for unrecognized users. Similarly, **ANZAI** additionally fails to teach or suggest Applicant's particularly claimed enablement of a predetermined minimum level of functionality/setting options for unrecognized users. For example, whereas **ANZAI** discloses a keyless vehicle operation identification and authorization system which enables **different users** to have different levels of authorization, **unrecognized users** of the **ANZAI** system are **denied access**. See, for example, Fig. 5 of **ANZAI**, decision box S3, box S9 and box S11; Fig. 6 of **ANZAI**, decision box S19, box S27 and display box S29; or Fig. 7 of **ANZAI**, decision box S43, box S49 and display box S51.

For example, col. 6 of **ANZAI**, lines 28 - 34 states:

> "The processor 29 and CPU 33 determine whether the user is authorized at Step S3. If the user is authorized, a first tone is provided at Step S5 and the vehicle doors are unlocked at Step S7. If at Step S3 it is determined that the user is not authorized, then a second tone is generated at Step S9 **and entry is denied at Step S11. The system then returns to its initial condition.**" [emphasis added by Applicant]

See also **ANZAI**, col. 6, lines57 - 60 and col. 7, lines 22 - 25. Again, the denial of access to unrecognized users in

ANZAI, even with the vehicle operating a tone and a display (which are not the **enabling** of a predetermined minimum level of functionality **for** unrecognized users), is not analogous to Applicant's claimed **enablement of a predetermined minimum level of functionality/setting options for unrecognized users.** Like **TUOMELA**, **ANZAI** is a binary system when it comes to denying access to unrecognized users.

As such, and for other reasons not argued herein, all of Applicant's claims are believed to be patentable over **TUOMELA** and/or **ANZAI**, alone, or in combination.

Nor do the further references of **HARIF** or **HARKIN**, cited in combination with **TUOMELA** in the Office Action against certain dependent claims, cure the deficiencies of **TUOMELA** and **ANZAI**. For example, **HARIF** discloses a keyed authentication system, wherein if authentication of the key cannot be made, and the key does not, on its own, unlock the door mechanically, then access is denied. See **HARIF**, paragraph [0051]. In fact, **HARKIN** teaches that, in such a case where the key mechanically may open a lock, but the authorization may have expired, the system may be further **disabled**. See **HARIF**, paragraph [0071], which states:

> "As long as they have the appropriate programmed key and insert it into the correct lock, entrance may be granted. Alternatively, in conjunction with

> traditional biometric or keypad authentication methods, the keyed authentication system may provide another level of security. **For example, the system may include a rule set such that if an unauthorized programmed key is used to gain access, the authentication device may trigger the key disabling logic and disable the biometric or keypad authentication means.** In other words, once the programmable key invalidates the security system, no code orbiometric feature would suffice to grant access." [emphasis added by Applicant]

See also, **HARIF**, paragraph [0070].

The **HARKIN** reference discloses a hand biometrics sensing device, but merely states on the subject of recognition, in col. 8, lines 1 - 7:

> "Data from the circuit 61 is supplied to a computer 62 which through standard algorithms compares the data with biometric characteristical data of a plurality of hands, or a single hand depending on whether the system is used for identification or merely verification purposes, held in a storage device 63 **and which provides an output in accordance with whether or not a match has been found**." [emphasis added by Applicant]

As such, it is believed that the cited references **TUOMELA, ANZAI, HARIF** and **HARKIN**, fail to teach or suggest Applicant's particularly claimed invention, individually, as well as together, in combination.

It is accordingly believed that none of the references, whether taken alone or in any combination, teach or suggest the features of claims 1 and 29. Claims 1 and 29 are,

therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claims 1 or 29. As it is believed that the claims were patentable over the cited art in their original form, the claims have not been amended to overcome the references.

Finally, Applicant appreciatively acknowledges the Examiner's statement that claims 15, 16 and 22 -28 "would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." In light of the above, Applicants respectfully believe that rewriting of claims 15, 16 and 22 -28 is unnecessary at this time.

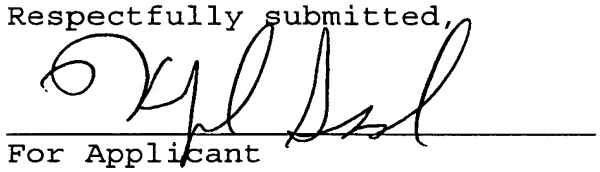
In view of the foregoing, reconsideration and allowance of claims 1 - 34 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate receiving a telephone call so that, if possible, patentable language can be worked out.

If an extension of time for this paper is required, petition for extension is herewith made.

Please charge any fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,



Kerry P. Sisselman
Reg. No. 37,237

For Applicant

August 9, 2005

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101